

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-263383

(43)Date of publication of application : 11.10.1996

(51)Int.Cl. G06F 12/14  
G06F 15/00

(21)Application number : 07-060952

(71)Applicant : HITACHI LTD

(22)Date of filing : 20.03.1995

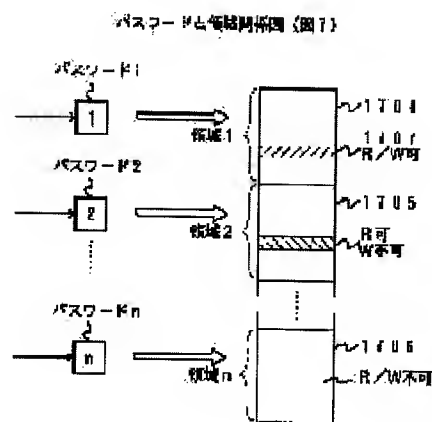
(72)Inventor : OGAWA HITOSHI  
NISHINA MASATOSHI  
MIYAZAWA SHOICHI

## (54) INFORMATION PROCESSOR

### (57)Abstract:

**PURPOSE:** To prevent data from being stolen by permitting the access to a unit corresponding to an accepted password in a first correspondence relation and the access to a specific unit corresponding to a password other than the accepted password in a second correspondence relation at the time when the accepted password coincides with a stored password.

**CONSTITUTION:** Passwords 1 to (n) correspond to independent areas 1704 to 1706 out of storage areas of a magnetic disk in 1:1. Areas 1704 to 1706 are sets of plural units each of which is a collectively stored information file. The user who knows the password can set an area 1707, which information read out of and write to are permitted to another user who knows one of the other passwords 2 to (n), in a part of the area 1704. For the purpose of preventing the wrong read of data, the user preliminarily determines and registers the upper limit or the number of set passwords and must input another set password.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平8-263383

(43) 公開日 平成8年(1996)10月11日

(51) Int.Cl. <sup>6</sup>	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 12/14	3 2 0		G 0 6 F 12/14	3 2 0 C
15/00	3 3 0	9364-5L	15/00	3 3 0 B

審査請求 未請求 請求項の数12 O L (全 17 頁)

(21) 出願番号 特願平7-60952

(22) 出願日 平成7年(1995)3月20日

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 小川 仁

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(72) 発明者 仁科 昌俊

神奈川県小田原市国府津2880番地 株式会

社日立製作所ストレージシステム事業部内

(72) 発明者 宮沢 章一

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(74) 代理人 弁理士 富田 和子

(54) 【発明の名称】 情報処理装置

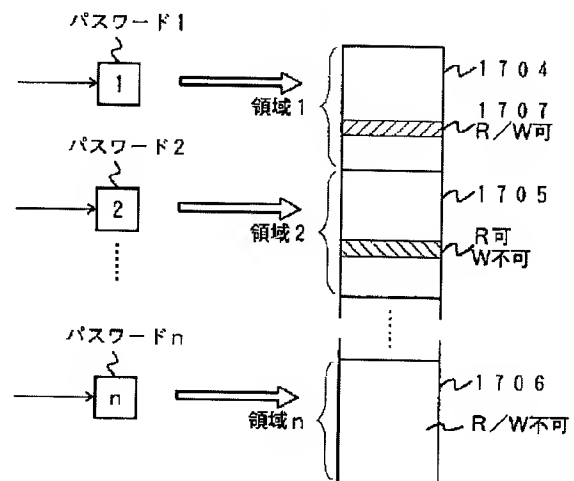
(57) 【要約】

【目的】 複数のユーザで共有した場合、互いのユーザがパスワードを公開することなく、しかも、データを共有できる情報処理装置を提供する。

【構成】 複数のパスワード1～nを設定する。各パスワードは、情報格納部のそれぞれ独立の情報の単位に対応させ、これを管理させる。一方で、情報の中の特定の領域1707は、直接対応していない他のパスワード2～nとも対応させておく。そして、この領域1707には、他のパスワード2～nによっても、アクセスが可能な構造である。

【効果】 複数の人の装置を共有しても、不正なユーザにデータ窃盗される可能性が低下する。

パスワードと領域関係図 (図7)



## 【特許請求の範囲】

【請求項 1】情報を格納する情報格納部と、前記情報格納部にひとまとまりに格納されている情報を単位として、前記単位に 1 対 1 で対応する複数のパスワードの第 1 の対応関係を示す情報、および、前記単位の中の一部の特定の単位と前記パスワードのうち対応していない他のパスワードとの第 2 の対応関係を示す情報を格納する第 1 の関係格納部と、外部から入力されるパスワードを受け付けるための第 1 の受け付け部と、前記受け付け部が受け付けたパスワードと前記複数のパスワードのいずれかとが一致する場合、前記一致するパスワードに前記第 1 の対応関係により対応する単位へのアクセス、および、前記一致するパスワード以外の他のパスワードに前記第 2 の対応関係により対応する単位の中の前記特定の単位へのアクセスを許可する第 1 の制御部とを有することを特徴とする情報処理装置。

【請求項 2】請求項 1 において、前記単位は、前記情報格納部に格納される情報の論理的なアドレス、物理的なアドレス、および、情報のまとまりのうちのいずれかであることを特徴とする情報処理装置。

【請求項 3】請求項 1 において、前記受け付け部が前記他のパスワードを受け付けた場合に、前記特定単位への書き込み動作を許可することを示す情報、読み出し動作を許可することを示す情報、および、その両動作を許可することを示す情報のうちのいずれかの情報を格納する第 2 の関係格納部をさらに有し、前記第 1 の制御部は、前記アクセスとして、前記第 2 の関係格納部に格納されている情報の動作を許可することを特徴とする情報処理装置。

【請求項 4】請求項 3 において、前記第 1 の関係格納部には、複数の特定単位が格納され、前記第 2 の関係格納部は、前記特定の単位ごとに、当該特定単位への書き込み動作を許可することを示す情報、読み出し動作を許可することを示す情報、および、その両動作を許可することを示す情報のうちのいずれかの情報を格納することを特徴とする情報処理装置。

【請求項 5】請求項 1 において、前記第 1 の対応関係を示す情報、および、第 2 の対応関係を示す情報を外部から受け付けるための第 2 の受け付け部をさらに有し、前記第 2 の受け付け部が受け付けた第 1 の対応関係および第 2 の対応関係を示す情報を、前記第 1 の関係格納部に格納するための第 2 の制御部をさらに備えることを特徴とする情報処理装置。

【請求項 6】請求項 1 において、前記第 1 の制御部は、第 1 の受け付け部が受け付けたパスワードと前記複数のパスワードとが不一致である場合、その回数を計数し、前記回数が予め定めた回数を超えた場合、それ以降の前記情報格納部へのアクセスを禁止することを特徴とする情報処理装置。

【請求項 7】請求項 1 において、前記第 1 の受け付け部は、前記パスワードと前記単位とを受け付け、前記第 1 の制御部は、前記第 1 の受け付け部が受け付けたパスワードと単位とが、前記第 1 の対応関係と一致する場合に限って、前記アクセスを許可することを特徴とする情報処理装置。

【請求項 8】請求項 7 において、前記第 1 の制御部は、第 1 の受け付け部が受け付けたパスワードと単位とが、前記第 1 の対応関係と不一致である場合、その回数を前記単位ごとに計数し、前記回数が予め定めた回数を超えた場合、それ以降の前記情報格納部へのアクセスを禁止することを特徴とする情報処理装置。

【請求項 9】請求項 1 において、当該情報処理装置の管理権の所在を特定するための情報を格納する管理権情報格納部と、指示を受けた場合に、前記管理権情報を出力する第 3 の制御部とをさらに有することを特徴とする情報処理装置。

【請求項 10】請求項 6 または 8 において、前記禁止の状態を保持する保持部をさらに有し、前記保持部が禁止状態を保持している場合、前記アクセスの禁止を報知するための報知手段をさらに有することを特徴とする情報処理装置。

【請求項 11】請求項 1 において、前記情報格納部に格納すべき情報を受け付けるための第 3 の受け付け部と、外部から符号を受け付けるための第 4 の受け付け部と、前記第 3 の受け付け部が受け付けた情報を、第 4 の受け付け部が受け付けた符号によって、暗号化して、情報格納部に格納する情報書き込み部と、前記第 4 の受け付け部が受け付けた符号によって、前記情報格納部の情報を、復号化して読み出すための情報読み出し部とをさらに有することを特徴とする情報処理装置。

【請求項 12】請求項 11 において、前記情報書き込み部は、書き込みを行う部分が、前記特定の単位であるかどうかを判定し、前記特定の単位である場合には、暗号化を禁止することを特徴とする情報処理装置。

## 【発明の詳細な説明】

## 【0001】

【産業上の利用分野】本発明は、ディスク装置などの情報処理装置に関し、特に、正当なユーザ以外へのデータの漏洩防止する手段を備えた情報処理装置に関する。

## 【0002】

【従来の技術】ディスク装置は、近年、小型化、高速化、高機能化、および、低価格化が急速に進んでいる。現在では、1. 8 インチのメモ리카ード型（高さ 10 mm 程度）、1. 3 インチのメモ리카ード型が製品化されている。また、ディスク装置のインタフェースも SCSI (Small Computer System Interface), PCMCIA (Personal Computer Memory Card International Association), I

DE (Intelligent Drive Electronics) などの標準インタフェースの普及が進んでおり、誰でも気軽にディスク装置をホストに装着して使用することが可能になってきている。製品としてもディスクパックとして、抜き差し可能なディスク装置が販売されている。

【0003】また、PCMCIAインタフェースを持った1.8インチディスク装置では、フロッピー感覚でディスク装置を使うことが可能となりつつある。このようなディスク装置では、ホストが同一の場合では特に、ディスク装置の互換性が高い。

【0004】ところで、ディスク装置の記憶容量は年々急激に伸びている。例えば、2.5インチディスク装置でも、記憶容量が1GBに達する勢いである。これにより、数年前のワークステーションクラスの装置の記憶容量が、ポケットに入る程度の大きさのディスク装置で得ることができるようになりつつある。また、同時に、このような大容量のディスク装置が、個人で所有され、個人データ管理に使えるようになってきている。

【0005】個人で所有されたディスク装置は、気軽に自分のホストに装着してデータを読み書きできるが、多量のデータの中には、他人に知られては困る個人データなどが保存されていることもある。したがって、気軽にディスク装置のデータを読み書きが自由に出来ると、不正にデータを窃盗されたり、データの破壊を試みるものが出てくる可能性がある。現在、小型ディスク装置は、万人に使用できる方向に進んできているが、ディスク装置の保存データの保全のための対策は、十分とはいえない。

【0006】しかし、最近、パスワードを設定できる2.5インチディスク装置が発売された。この装置は、正しいパスワードを入力出来ないユーザに対して、ディスク装置のデータの読み出し／書き込みに関するコマンド制限を行っている。また、不正ユーザがパスワード破りを電源投入期間中に5回間違えるとアクセス不可にする機構も含まれている。

【0007】また、特開平4-360068号公報では、格納すべきデータを、解読困難な符号化データに加工してから格納する記録再生装置が提案されている。また、特開昭62-154190号や、特開平1-118980号公報では、予め暗証番号を登録し、誤った暗証番号を予め定めた回数入力すると、データを読みだし不能にする記憶装置がそれぞれ開示されている。

【0008】

【発明が解決しようとする課題】上記従来のディスク装置等の情報処理装置では、パスワードや暗証番号が不明な場合、情報処理装置の媒体からのデータ読み出し／書き込みが全くできないため、持ち主が、他人に対してデータの読み書きを許可する場合、パスワードを他人に教えなければならない。しかしながら、パスワードを教え

ることによって、パスワードの効果が薄れたり、パスワードを開放することによって、パスワードを設定していない装置と同じになるため、どちらにしてもデータの窃盗からデータを保全することが難しくなるという問題があった。

【0009】本発明は、複数のユーザで共有可能でありながら、データの窃盗を防止することのできる情報処理装置を提供することを目的とする。

【0010】

【課題を解決するための手段】上記目的を達成するために、本発明によれば、情報を格納する情報格納部と、前記情報格納部にひとまとまりに格納されている情報を単位として、前記単位に1対1で対応する複数のパスワードの第1の対応関係を示す情報、および、前記単位の中の一部の特定の単位と前記パスワードのうち対応していない他のパスワードとの第2の対応関係を示す情報を格納する第1の関係格納部と、外部から入力されるパスワードを受け付けるための第1の受け付け部と、前記受け付け部が受け付けたパスワードと前記複数のパスワードのいずれかと一致する場合、前記一致するパスワードに前記第1の対応関係により対応する単位へのアクセス、および、前記一致するパスワード以外の他のパスワードに前記第2の対応関係により対応する単位の中の前記特定の単位へのアクセスを許可する第1の制御部とを有する情報処理装置が提供される。

【0011】

【作用】本発明の情報処理装置は、複数のパスワードが設定できる。各パスワードには、情報格納部の情報格納領域が、1対1で対応する。この関係は、第1の関係格納部に第1の対応関係として格納されている。第1の受け付け部に入力されたパスワードが、前記複数のパスワードのいずれかと一致する場合、一致するパスワードへ対応する情報格納領域への情報の書き込みおよび読み出しのうちの少なくとも一方の動作が、第1の制御部により許可される。

【0012】また、前述の情報格納領域の中には、特定の領域が設定される。この特定の領域は、第1の対応関係で対応しているパスワードが入力された場合以外に、複数のパスワードのうちの他のパスワードが入力された場合に、特定領域に格納されている情報の書き込みおよび読み出しのうちの少なくとも一方の動作、第1の制御部により許可される。

【0013】したがって、本発明の情報処理装置を複数のユーザで共有する場合、各ユーザがパスワードを設定することにより、ユーザ間において情報を公開することなく、秘密にすることができる。しかも、複数のユーザ間で、共有したい情報については、自分のパスワードに対応する領域のなかに特定の領域を設定し、この特定の領域に格納することにより、他のパスワード知っているユーザは、この情報を知ることができ、情報の共有化が

実現できる。しかしながら、複数のパスワードのいずれも知らない不正ユーザは、この特定の領域の情報を、読み書きすることができないため、特定領域の情報が公開されるわけではなく、情報が窃盗させることを防止できる。

#### 【0014】

【実施例】以下、本発明の一実施例のディスク装置について、図面を用いて説明する。

【0015】本実施例のディスク装置107は、外形がクレジットカードと同等の大きさの超薄型ディスク装置である。ディスク装置107は、ホストインタフェース108を介して、ホストコンピュータ109に接続される(図1、図2)。

【0016】本実施例のディスク装置の構成についてさらに説明する。

【0017】ディスク装置107は、図1のように、機構部100と電子回路部105とを備えている。本実施例では、この電子回路部105に、ディスク装置の所有者を表す所有者特定情報を格納する部分およびパスワードを格納する部分を設けている。具体的には、本実施例では、電源遮断時でも記憶情報を忘れないためにフラッシュメモリ106に上記情報を格納している。

【0018】機構部100は、図5のように、データを読み書きするためのヘッド101、ユーザデータを保存するための磁気ディスク102、ヘッドを駆動するためのモータであるVCM(Voice Coil Motor:ボイスコイルモータ)103、媒体を回転するためのスピンドルモータ104とを備えている。

【0019】電子回路部105は、図5のように、CPU505と、機構制御部511と、ヘッド101との間で記録再生するデータの受渡しおよび受け取りを行う記録/再生回路501と、データ処理部502と、磁気ディスク102から読み出したデータを一時的に留め置くデータバッファ509とを備えている。

【0020】機構制御部511およびデータ処理部502は、CPU505のシステムバス11に接続されている。機構制御部511とヘッド101とは、制御線12によって接続されている。機構制御部511は、制御線12を介して、機構部100に、機械的な動作を制御する信号を出力する。記録/再生回路501は、ヘッド101と、データ線13によって接続され、ヘッド101に記録すべきデータ信号を受渡し、ヘッドが再生したデータ信号を受け取る。記録/再生回路501と機構制御部とは、制御線14によって接続されている。データ処理部502とデータバッファ509とは、データバス15によって接続されている。

【0021】データ処理部502の構成を更に説明する。データ処理部502は、CPUインタフェースコントロール部504と、ホストインタフェースコントロール部510と、ドライブインタフェースコントロール部

503と、バッファコントロール部と、読みだし誤り検出情報(ECC)処理部506とを備えている。CPUインタフェースコントロール部504、ホストインタフェースコントロール部510、および、ドライブインタフェースコントロール部503は、内部制御バス16に接続されている。バッファコントロール部507、ホストインタフェースコントロール部510、ドライブインタフェースコントロール部503、および、ECC処理部506は、データバス17によって接続されている。

【0022】ホストインターフェースコントロール部510には、内部にコマンドレジスタ521とエラーレジスタ522とが配置されている。また、バッファコントロール部507には、内部に、データを加工するためのキーワードを格納するキーワード格納部508が設けられている。

【0023】本実施例のディスク装置は、磁気ディスク102に格納されているデータが不正に読み出されることを防止するためのシステムと、ディスク装置の所有者を示すためのシステムが備えられている。これについて説明する。

【0024】本実施例のディスク装置107では、図7に示すように、データが不正に読み出されることを防止するために、パスワードを設定することができる。パスワードは、フラッシュメモリ106に格納される。パスワードは、磁気ディスク102に格納されているデータをアクセスするための許可を与えるものである。本実施例では、データが不正に読み出されることを防止しながらも、複数の人が、ディスク装置を共用することを可能にするために、複数のパスワードが設定可能な構成である。

【0025】具体的には、図7のように、n個のパスワード1~nが設定可能である。各パスワード1~nは、磁気ディスク102の記憶領域のうち、それぞれ独立の領域1704~1706と、1:1で対応する。領域1704~1706は、ひとまとまりに格納される情報ファイルを単位し、複数の単位の集合である。領域1704~1706にアクセスするためには、対応するパスワードを入力しなければならない。従って、パスワード1に対応する領域1704には、基本的には、対応するパスワード1を入力しなければ書き込みも読み出しもできない。

【0026】しかし、パスワード1を知るユーザは、他のパスワード2~nのいずれかを知っているユーザに対して、情報の読み出し/書き込みを許可する領域1707を、領域1704内の一部に設定することができる。この領域1707も、上述の単位の集合である。また、読み出し/書き込みの許可以外に、書き込みのみの許可、および、読み出しのみを許可する領域を設定することができる。これらの領域の情報は、フラッシュメモリ106に格納される。

【0027】また、本実施例では複数のパスワードが設定可能であるが、パスワードの追加／削除を、誰もが自由に行えると、ディスク装置を拾得したような不正なユーザが、パスワードを新たに設定できるため、上述の領域1707のような領域の情報を読みだされる恐れがある。したがって、データが不正に読みだされることを防止するためにパスワードを設定している意味がなくなるので、パスワードの設定数の上限をユーザが予め決めて登録するか、パスワードを新たに設定するためには、既に設定されている他のパスワードを入力しなければならないような構成にする必要がある。本実施例では、パスワードの設定数の上限を予め定める構成である。

【0028】フラッシュメモリ106に格納される所有者特定情報について説明する。

【0029】所有者特定情報は、本実施例のディスク装置107の所有者を特定するための情報である。この情報は、ホスト109から入力し、フラッシュメモリ106に格納する。所有者特定情報としては、たとえば、所有者名や住所、電話番号、電子メール(E-mail)の宛先等を用いることができる。所有者特定情報は、パスワードにかかわらず読み出せる構成である。ユーザは、ディスク装置をホストに装着したとき、パスワードを入力する前に、この所有者特定情報を読み出して、ホストの表示装置に表示させることで、どのディスク装置かを特定することができるための、どのパスワードをいれたらよいかきめるための参考になる。ただし、パスワードが一致するまでは、所有者特定情報の内容の変更を許さない構成である。これにより、ホストにディスク装置を装着したとき、パスワードに関わりなく、どのディスク装置かがユーザには認識できるようになる。また、このような構成にすることにより、ディスク装置を拾得した人が、パスワードに係わりなく所有者特定情報を読み出すことができるので、ディスク装置の持ち主が特定できるという効果も得られる。

【0030】フラッシュメモリ106内に格納されている情報を、図8を用いて説明する。フラッシュメモリ106には、パスワード1～nに関する情報を格納する領域1801、1802、1810と、上述の所有者特定情報領域1811と、パスワード破りが試みられたことを示すフラグを格納する領域とを備えている。このように、パスワードに関する情報、所有者特定情報、および、パスワード破りを示すフラグをフラッシュメモリ106のような不揮発メモリに格納することにより、電源を落してもこれらの情報が失われることがない。また、不揮発メモリに限らず、電源を落しても情報が消えないバックアップ付きメモリ、例えば、SRAMや、ディスク102に保存する構成にすることももちろん可能である。

【0031】パスワード1に関する情報を格納する領域1801は、パスワード1を格納する領域1803と、

後で説明するようにパスワード1の入力をミスした回数を格納する領域1804と、パスワード1に対応するディスク102の領域の位置情報を格納する領域1805、1807等と、その領域について、他のパスワード2～nを知るユーザに読み書きを許可するかという属性を格納する領域1806、1808等に分けられている。

【0032】図8に示した一例では、ディスク102のLBA0～1000、1001～2000等が、パスワード1に対応する領域である。但し、LBA(Logical Block Address)は、論理的な番地を表す。LBA0～1000の領域は、他のパスワード2～nを知るユーザに書き込みを許可する。LBA1001～2000の領域は、他のパスワード2～nを知るユーザであっても、読み出し／書き込みを許可しない。

【0033】つぎに、本実施例のディスク装置の動作について、説明する。

【0034】本実施例のディスク装置は、図2のように、ホスト109と接続される。CPU505は、図9のように、ホスト109よりコマンドを受け取る(ステップ1901)。このコマンドは、ディスク装置とホスト109とのデータのやり取りのプロトコルに従って送られてくる。具体的には、図9に示す様に、ホスト109が、ホストインタフェースコントロール部510内のコマンドレジスタ521内に、コマンドを書き込むことにより行う。インタフェース108として、一般的なIDEを用いる場合、コマンドレジスタ(アドレス1F7h)にホスト109がコマンドを書き込む。何もホスト109より指示がこなかった場合、指示待ちとなる。

【0035】次に、コマンドレジスタ521にコマンドが書き込まれると、データ処理部502からCPU505に割り込みをかけ、コマンド内容の解釈をCPU505が行う(ステップ1902)。コマンドの解釈後、パスワード破りがされていないか、フラッシュメモリ106の領域1812のフラグをチェックする(ステップ1903)。

【0036】パスワード破りが行われていれば、パスワード破り処理へ移る。パスワード破りがされていないければ、ステップ1902で解釈したコマンドが、パスワード設定コマンドである場合には、以下パスワードを設定するための動作を行う。パスワード設定コマンドでなければ、そのコマンドの処理に移る(ステップ1904)。

【0037】パスワード設定のための処理である場合、まず、フラッシュメモリ106に格納されているパスワードの個数を調べ、この個数と、フラッシュメモリ106に格納されている、あらかじめ定められたパスワード上限数と比較する(ステップ1905)。パスワードの上限数の設定のための動作については、後で述べる。

【0038】パスワード数が、上限数に達していないならば、データバッファ内に格納されているパスワード、および、そのパスワードに対応する領域の領域分け情報およびその属性をCPU505に取り込む（ステップ1906）。フラッシュメモリ106に格納されているパスワードの個数が、すでに上限数に達している場合には、新たにパスワードを設定することができないので、エラーレジスタ522に、パスワード上限数を超えるというエラーステータスをセットし、ホストに表示させる。

【0039】このデータバッファ509内に格納されているパスワード、および、その領域分け情報等は、ホスト109が、ステップ1901でコマンドを書き込む時に、ホスト109によって、データバッファ509に書き込まれる。データバッファ509に格納される情報は、具体的には、設定するパスワードと、そのパスワードに対応するディスク102の領域内の領域分けと、その領域分けした領域に設定する属性（他のパスワードを知っているユーザに読み出しおよび書き込みを許可する、読み出しのみを許可する、書き込みのみ許可する、読み出しも書き込みも許可しないのうちのいずれか）である。

【0040】つぎに、ステップ1906で取り込んだパスワードが、既にフラッシュメモリ106に格納されている他のパスワードと重複していないかどうか比較を行い、重複がある場合、エラーレジスタ522に、設定したパスワードが重複しているというエラーステータスをセットし、ホスト109に表示させる（ステップ1908）。重複がなければ、フラッシュメモリ106の空いている領域、例えば領域1803（図8）にパスワードを格納する（ステップ1909）。また、データバッファから取り込んだ領域分けした領域間に重複がないか判断し、重複があれば、エラーレジスタ522に領域重複のエラーステータスをセットし、ホストに表示させる（1910）。重複がなければ、フラッシュメモリ106の領域1804から1808等に、領域分け格納を同様に行う（ステップ1911）。以上により、ディスク装置へのパスワード設定、領域設定が実現できる。

【0041】つぎに、パスワードの上限数、および、各パスワードに対応するディスク102の領域範囲を設定する動作について、説明する。

【0042】図9のステップ1901で、ホスト109より、コマンドレジスタ521とデータバッファ509にコマンドとパラメータが来た場合、ステップ1902でコマンド解釈する。ここで、送られて来たコマンドが、パスワード設定コマンドでない場合（ステップ1904）、図10のステップ2001に進む。ステップ2001では、コマンドがパスワード上限数と領域とを設定するためのコマンドである場合、パスワード上限数および領域が、フラッシュメモリ106にすでに設定され

ているかどうか調べ、設定されているならエラーとする（ステップ2002）。設定されていないならば、データバッファ509よりパラメータの読み込みをCPUが行う（ステップ2003）。ここで、パスワード上限数を設定するコマンドであるなら、データバッファ509には、ホスト109から、図10に示すように、パスワード上限数と、各パスワードに対応するディスク102の領域がホストより格納されている。CPU505は、これらをデータバッファ509より読み込み、設定されている領域間で重複がないかどうかチェックし、重複があるなら、エラーレジスタ522にエラーステータスをセットし（ステップ2005）、重複しなければ、パスワード数と、対応させる領域とを、フラッシュメモリ106に格納する（2006）。以上により、パスワード数、領域範囲設定が実現できる。

【0043】つぎに、パスワードを解除して、ディスク102のデータを読み出し／書き込みする動作について説明する。

【0044】図10のステップ2001において、図9のステップ1902で解釈したコマンドが、パスワード上限数設定コマンドでない場合、図11のステップ1300に進む。そして、ディスク102のデータを読み出しましたは書き込みするコマンドである場合、データバッファ509にホスト109が書き込んだ、パスワードを解除したい領域を取り込む（ステップ1301）。

【0045】つぎに、データバッファ509にホスト109が書き込んだパスワードを、CPU505が取り込む（ステップ1302）。そして、ステップ1301で取り込んだ領域に対応する正しいパスワード（例えば、図8のパスワード1）をフラッシュメモリ106から読みだし、ステップ1302でホストから設定されたパスワードと比較する。そして、このパスワードが一致する場合、正当なユーザであると判断し（ステップ1303）、フラッシュメモリ106のパスワード1のミス回数を格納する領域1804を0に戻す（ステップ1308）。

【0046】そして、ホスト109に本当に解除したいかどうか確認し、確認がとれたならば、パスワード1に対応するディスク102の領域（図8のフラッシュメモリの1805、1807に格納されている領域）のデータ読み出しおよび書き込みを可能にする。また、パスワード1に対応する領域以外に、他のパスワード2～nに対応する領域の中で、フラッシュメモリ106に読み出し可能、書き込み可能、および、読みだし／書き込み可能ないずれかの属性が設定されている領域については、その属性の動作を可能にする。

【0047】一方、ステップ1303で、ホスト109から入力されたパスワードが、正しくない場合、フラッシュメモリ106の該当するパスワードのパスワードミス回数格納領域1804に格納されている回数を+1す

10

20

30

40

50

る。そして、この回数が、予め定めた回数以上である場合、不正なユーザがパスワード破りを試みていると判断し、フラッシュメモリ106の領域1812にパスワード破りを示すフラグを立て、動作を終了する(ステップ1309、1304、1305)。したがって、ディスク102への読み書きは実行しない。これにより、不正ユーザがパスワード破りを行おうとしても、予め定めた回数以上は、パスワードを入力できない。

【0048】また、ステップ1307で正しいパスワードが入力され、読みだし/書き込みが可能になった場合、データの読み出し/書き込みの動作を実行する。

【0049】具体的には、読み出しを行う場合には、CPU505は、ディスク102の該当セクタのデータのリードを行うために、機構制御部511に指示する。機構制御部511は、CPUの指示に従い、ヘッド101をディスク102の該当トラックに位置づける。これにより、該当セクタのデータ読み出しが行われ、記録/再生回路501で、アナログ信号がNRZ(Non Return to Zero)信号に変換される。この信号が、データ処理部502のドライブインタフェースコントロール部503に取り込まれる。

【0050】次に、読みだしたデータは、読みだしデータのエラーチェックを行なうためのECC処理部506と、バッファコントロール部507を経由して、データバッファ509に送られる。そして、ECC処理部506でエラー発生無しと報告されると、データバッファ509に格納されていた読み出しデータが、ホストインタフェースコントロール部510を経由して、ホストに転送されていく。ディスク102へのデータの書き込みも同様であるので説明を省略する。

【0051】また、データの読みだし、書き込み時に、データを加工して暗号化することが可能である。これにより、不正なユーザに、データを盗まれる可能性がさらに低減する。データの加工方法については、後で述べる。

【0052】つぎに、フラッシュメモリ106に所有者特定情報を格納または消去するための動作について説明する。

【0053】図9のステップ1902で解釈したコマンドが、図10のステップ2001でパスワード上限数設定コマンドではなく、さらに、図11のステップ1300において、データの読み出し/書き込みコマンドでもない場合、図16のステップ1600に進む。ここで、所有者特定情報登録/消去コマンドである場合、フラッシュメモリ106の領域1811に格納されている情報を消去してよいかどうかをホスト109に表示させてユーザに確認する(ステップ1601)。消去してよい場合、所有者特定情報を登録するかどうか、ホスト109に表示させてユーザに確認する。登録する場合、ホストより登録すべき所有者特定情報が入力され、これをフラ

ッシュメモリ106の領域1811にオーバーライトする。登録しない場合、すでに格納されている所有者特定情報の消去のみを行う(ステップ1602、1603、1604)。

【0054】一方、図9のステップ1903で、フラッシュメモリ106の領域1812にパスワード破りのフラグがたっていた場合、図12のステップ2201に進み、パスワード破りが行われたことをホスト109に表示させる。この表示は、ホスト109の表示装置に、パスワード破りが行われたことを表示させる方法以外に、例えば、ホスト109やディスク装置自体に予めLEDを取り付けておき、このLEDを点滅させる方法を用いることができる。また、ホスト109に音声発生装置が備えられている場合には、この音声発生装置によって、パスワード破りが行われた旨をユーザに報知する方法を用いることができる。

【0055】つぎに、図9のステップ1902で解釈したコマンドが、予め定められたコマンドであるかどうか判断する。そして、予め定められた、受け付けるコマンドである場合には、図13に移り、その処理を行うが、受け付けないコマンドである場合には、エラーレジスタにエラー発生とエラーステータスを設定し、ホストにエラー発生を知らせる(ステップ2202、2203)。

【0056】ステップ2202で受け付けるコマンドは、ディスク102に格納されているデータが不正なユーザに盗まれる恐れのない動作を行うためのコマンドである。受け付けないコマンドは、データが盗まれたり、不正に書き替えられたりする恐れのある動作を行うためのコマンドである。

【0057】以下、ステップ2202で受け付けるコマンドの例と受け付けないコマンドの例とを示す。

【0058】受け付けるコマンドの例は、つぎの通りである。

【0059】・所有者特定情報を表示させるためのコマンド

・パスワード破りの状態を復帰させるためのコマンド

・データの転送を伴わないコマンド群(Non-Data)

例えば、ホスト109が、1トラック当たりのセクタ数、および、シリンダ当たりのヘッド数を設定するイニシャライズ ドライブ パラメーターズ(Initialize Drive Parameters)、ホスト109へのデータの転送を伴わないリードおよびベリファイを行うリード ベリファイ(Read Verify)、シリンダ0へのシークを行うリキャリブレート(Recalibrate)、指定されたトラックとヘッドに対してシークを行うシーク(Seek)、ベンダユニークコマンドを設定を行うセット フィーチャーズ(Set Features)、ディスク装置に自己診断を行うエグゼキュートドライブ ダイアグノスティック(Execute drive diagnostic)。

## 【0060】・パワーコマンド群

例えば、ディスク装置のパワーモードを報告するチェック パワー モード (Check Power Mode)、ディスクの回転をアイドルモードに移行させ、割込みを発生させるアイドル (Idle)、ディスクの回転をアイドルモードに移行させ、即座に、割込みを発生させるアイドル イミディエイト (Idle Immediate)、ディスクの回転を停止させるスリープ (Sleep)、ディスクの回転をスタンバイモードに移行させ、割込みを発生させるスタンバイ (Standby)、ディスクの回転をスタンバイモードに移行させ、即座に、割込みを発生させるスタンバイ イミディエイト (Standby Immediate)。

【0061】受け付けないコマンドの例は、つぎの通りである。

【0062】・パスワードおよび対応する領域を設定するためのコマンド

・パスワードおよび対応する領域を変更するためのコマンド

・所有者特定情報を設定するためのコマンド

・所有者特定情報を変更するためのコマンド

・ディスク装置からホストへのデータの転送を行うコマンド群

例えば、ディスク装置からパラメータ情報を受信するためのアイデンティファイ ドライブ (Identify Drive)、バッファ内の内容を読み取らせるリード バッファ (Read Buffer)、指定した数のセクタを読み取らせるリード セクタズ (Read Sectors)、指定した数のセクタを読み取らせ、エラー訂正コードとともに転送させるリードロング (Read Long)。

【0063】・ホストからディスク装置へのデータの転送を行うコマンド群

例えば、バッファにデータの書き込みを行うライト バッファ (Write Buffer)、指定した数のセクタが書き込まれるライト セクタズ (Write Sectors)、データとエラー訂正コードとを書き込むライト ロング (Write Long)、ディスクのフォーマットを行うフォーマットトラック (Format Track)。

【0064】つぎに、図12のステップ2202で受け付けたコマンドが、処理を受け付けるコマンドである場合、図13のステップ2301に進む。そして、ステップ2202で受け付けたコマンドがパスワード破り復帰コマンドであるかどうか判断し (ステップ2301)、復帰コマンドであった場合、ステップ2302で、データバッファ509にホストから書き込まれているパスワードを読み込む。そして、このパスワードが、フラッシュ106のパスワードミス回数1804が規定回数以上になっている、すなわちパスワード破りされたパスワ

ードであるかどうか判断する (ステップ2303)。そして、正しいパスワードである場合、ステップ2201 (図12) で表示させたパスワード破りの表示を停止させ (ステップ2304)、フラッシュメモリ106内の領域1812のパスワード破りのフラグをリセットする (ステップ2305)。

【0065】これにより、パスワード破りに対応するための動作が解除されるので、ステップ1901 (図9) で、データの転送を伴うコマンドを受け付けた場合、ステップ1904、および、図14のステップ2401を経て、該当コマンドを処理する動作を行うことができる。データの転送を伴うコマンドを処理する動作については、従来のディスク装置と同じであるので、説明を省略する。

【0066】また、図13のステップ2301で、データの転送を伴うコマンド群であった場合、図14のステップ2401を経て、該当コマンドを処理する動作を行う。

【0067】また、図9のステップ1902で解釈してコマンドが、図16のステップ1600で所有者特定情報登録/消去コマンドでない場合、または、図13のステップ2301でパスワード復帰コマンドでない場合には、図14のステップ2401に進む。そして、所有者特定情報を表示させるコマンドである場合、CPU505は、フラッシュメモリ106の領域1811に格納されている所有者特定情報を、データバッファ509にセットし (ステップ2402)、ホスト109へ、所有者特定情報をセットが終了したことを通達する (ステップ2403)。この通達は、ホスト109が見ることができる作業終了を示すステータスをセットするか、割込み信号線を使用してホストに知らせる方法を用いることができる。これにより、図2のように、ホストに所有者特定情報203が、表示される。

【0068】所有者特定情報の表示方法は、ホストの表示装置に限らず、ディスク装置に、表示部を設けておき、この表示部に表示させる方法を用いることも可能である。ディスク装置の表示部に表示させる場合、この表示部に常時所有者特定情報を表示させる構成にすることも可能である。また、ディスク装置に所有者特定情報を表示をユーザが要求するためのスイッチを設けておき、ホストから要求されたとき以外に、このスイッチが押下されたときに、一定時間ディスク装置の表示部に表示させる構成にすることも可能である。

【0069】上述の図11のステップ1310においてデータの読み出しや書き込みを行う際に、データの加工を行うことが可能である。これについて、説明する。

【0070】まず、バッファコントロール部507には、ホストよりあらかじめ、キーワードデータをキーワード格納部508に格納しておく。これによりバッファコントロール部507が、データバッファ509からデ

ータを読み出す順番を変更することや、書き込む順番を変更することができる。

【0071】例えば、データバッファ509にDRAMを使用した場合、通常、データを高速に読み出すために列アドレスを与えた後に、行アドレスのみ与えることで、データ16バイト程度、連続的に読み出せる高速ページモードを使用することが多い。この場合、上述のキーワードに従って、列アドレスを出す順番を変更することで、データバッファから、データを取り出す順番を変更する方法を用いることができる。また、読みだしデータとキーワードデータのEOR（排他的論理和）を取った後にデータをホストへ送るような方法を用いることができる。

【0072】これにより、データ書き込み時に指定したキーワードと読み出し時に指定したキーワードが一致しないと、ホスト109は、ディスク装置からデータを読み出せるが、このデータは解読できないデータとなる。従って、不正なユーザが、パスワードを見つけて、データを窃盗しようとしても、キーワードがわからないと、データとして意味をなさなくなる。これにより、さらにデータの保全性のよいディスク装置を提供することができる。

【0073】また、データの保全性をより高めるために、ホストインタフェースコントロール部510～データバッファ509間、データバッファ509～ドライブインタフェースコントロール部503間にデータをやり取りする際にキーワードを利用する回路を配置しておくこともできる。後者にキーワードを利用する回路を配置する場合、データ読みだし時のECC訂正が発生した場合、バッファ訂正アドレスの訂正位置を間違わないように注意する必要がある。

【0074】ただし、本実施例では、複数のユーザで、図7の特定領域1707の情報を共有する構成であるので、共有する領域1707の情報をユーザのうちのひとりがデータ加工して格納してしまうと、他のユーザは、その情報を読み出すことができなくなる。よって、複数のユーザ全員にキーワードを公開しなければならず、データ加工を行う意味が薄れてしまうので、本実施例においては、複数のユーザで共有する特定領域については、データ加工を禁止する構成にする。これは、データ加工を行う前に、書き込み領域がフラッシュメモリ106に格納されている特定領域であるかどうか判定し、特定領域である場合には、加工を禁止する構成にすることで実現できる。

【0075】図6、図17を用いて、上述のデータ加工方法についてさらに説明する。

【0076】ホスト109からデータ601をディスク装置に書き込む場合を例に上げて説明する。ホスト109よりあらかじめ、コマンドでキーワード格納部508にキーワードを格納しておく（ステップ1201）。図

6では、キーワードを8bitとして、0101 0100がセットされていたとする。この後、通常のデータライトでユーザデータ601がくると、ホスト109へデータ加工を行うかどうか確認をとる（ステップ1202）。そして、このデータ601をキーワード格納部508のデータとEORを取ったものを加工後のデータ602として、ディスク装置内で扱うとする（ステップ1203）。つまり、データバッファ509で1が立っているビットを反転する。図6のような回路をデータ処理部502内に設けておく。このようにすることで、ディスク装置からデータを読み出す時も、キーワード格納部508に、データ書き込み時と同じキーワードがセットされていないと、意味の無いデータになる。

【0077】これにより、例えばディスク装置のパスワード破りに不正ユーザが成功しても、次にキーワードが判らないかぎり、正当ユーザが知らないうちにデータを窃盗される可能性がたいへん低くなる。したがって、データの保全性のよいディスク装置が、簡単な回路構成で実現することができる。図6では、データ加工方法として、単純なEOR回路としたが、もちろん、もっと複雑なアルゴリズムにしてもデータを加工する目的なら、もちろんかまわない。

【0078】つぎに、列アドレスを出す順番を変更することによりデータ加工する方法を図3を用いて説明する。

【0079】図3、図15は、ホスト109からディスク装置へデータライト時のバッファ加工する方法を示す図である。

【0080】あらかじめ、データ処理部502にスキュー値格納部703を設けておく。そしてホスト109から、コマンドでスキュー値格納部703にスキュー値を格納しておく。

【0081】今、ホストより、ホストインタフェースコントロール部510に書き込みたいユーザデータ701が入ってきている。ここでは、一例として、512Byteあるとする。また、ホスト109へデータ加工を行うかどうか確認をとり、加工する確認がとれ、スキュー値の変更もない場合（ステップ1501、1502）、以下のように、スキュー値を用いてデータ加工を行う（ステップ1503）。

【0082】データバッファ509にはDRAMを使用しているとする。この場合、データを高速にデータバッファに読み書きするために、DRAMの1アクセス方式であるバーストモードを使用することが多い。これは、DRAMをアクセスする時、ロードアドレスを1回与えた後、カラムアドレスのみの変更、または、CASストロープの変更による自動アドレス変更機能で、データを高速にアクセスする機能である。これを実現するために、バッファコントロール部507内に配置されているバッファアドレス算出回路704、705で対応する。

【0083】ここでは、ローアドレス1回で、カラムアドレス変更16回のバースト転送モードを考える。この場合、ユーザデータ701を16Byte単位を1ブロック702とする。すると、512Byteは32個のブロックに分割できる。このデータをバッファに格納する時、ホストバッファアドレス算出回路704でバッファアドレスを算出するのであるが、この時スキュー値格納部703の値を利用する。今回は、2が入っていると、この2を利用して、データバッファ509には、図4に示すように、1ブロック飛ばしの順番で、データブロックを格納する。

【0084】これを、通常のバッファアクセスのように、ドライブバッファアドレス算出回路705が、バッファアドレスの上から順番に、ユーザデータを読み出すことで、ドライブI/Fコントロール部503へ送る。これにより、データの順番を入れ換えることによる、データ加工が実現できる。

【0085】さらに、図4は、データリード時のバッファ加工方式を示す図である。

【0086】動作は、図3に説明したのと逆になるだけであるので説明を省略する。

【0087】このようにすることで、データを読み出す時も、スキュー値格納部にデータ書き込み時と同じ値がセットされていないと、正しいデータとして読み出せない。したがって、たとえディスク装置のパスワード破りに不正ユーザが成功しても、次にスキュー値が判らないかぎり、正当ユーザが知らないうちにデータを窃盗される可能性がたいへん低くなる。よって、データの保全性のよいディスク装置が、簡単な回路構成で実現することができる。ここでは、ホストインタフェースコントロール部510とバッファインタフェースの間に、図3の回路を入れることを示したが、CRC/ECCの訂正のことも考慮すれば、バッファインタフェースとドライブインタフェースの間に、データ加工を行なう回路を入れることができる。また、今回は、データ加工方法として、単純なスキュー値によるブロックの順番の入れ換えの回路としたが、もちろん、もっと複雑なアルゴリズムにしてもデータを加工する目的なら、もちろんかまわない。

【0088】上述したように、本実施例のディスク装置では、1台のディスク装置に複数のパスワードを設定し、それぞれのパスワードに対応する領域を持たせる構成である。したがって、複数の人が各自のパスワードの管理領域でデータの読み書きをおこなっても、おたがい、自分のパスワードを公開する必要がない。

【0089】また、自分のパスワードの管理領域内に、他のパスワードを知っているユーザに対しての読み書きを許可する特定領域を設けることができるので、各ユーザ間のデータの共有化が可能である。

【0090】また、この特定の領域に対する他のユーザ

の動作の許可を、読みだしのみ、書き込みのみ、および、読みだしと書き込みのうちのいずれかに、特定の領域毎に設定することができる、格納する情報によって、必要な動作のみを許可でき、データの秘密を守ることをより確実に行える。

【0091】したがって、他人に自分のパスワードを教える必要がないため、自分の管理している領域のデータの機密を守りつつ、本人が公開したい情報だけ、公開したい人のみに公開することができ、データの保全性のよいディスク装置が実現できる。

【0092】また、パスワード入力ミスの回数管理、キーワードによる保存データの暗号化保存/復号化読み出し、不正使用者によるパスワード破り/暗号コード破りを試みられた場合のドライブ動作制限などを設けたことにより、本実施例のディスク装置は、他のディスク装置より保存データの不正ユーザによるデータ窃盗、データ破壊等に対して、信頼性が高い。

【0093】また、パスワード破りが行われたことを表示する構成であるため、正当使用者が、不正使用者にディスク装置がいじられたかどうかを知ることができる。

【0094】上述のディスク装置では、記録媒体として、磁気ディスクを用いたが、これに限らず、半導体メモリや光ディスク等の他の機種種類の記録媒体を用いることももちろん可能である。

【0095】さらに、本実施例では、パスワード数の上限と、各パスワードに対応する領域とを論理番地として、予め設定する構成であるが、パスワード数の上限のみを予め定め、ディスクに情報を入力する際に、その情報がどのパスワードに対応するかを定めるような構成にすることももちろん可能である。この場合、パスワードに対応する情報の特定を、論理番地の他、物理番地や、ファイル名、ディレクトリ等の情報単位で行うことももちろん可能である。

【0096】

【発明の効果】本発明によれば、複数のユーザで共有した場合にも、互いにパスワードを公開することなく、しかもデータを共有することのできる、情報処理装置が提供される。

【図面の簡単な説明】

【図1】本発明の一実施例のディスク装置の構成を示すブロック図。

【図2】本発明の一実施例のディスク装置をホストに接続する状態を説明する説明図。

【図3】図1のディスク装置でデータ加工を行う方法を示す説明図。

【図4】図1のディスク装置でデータ加工を行う方法を示す説明図。

【図5】図1のディスク装置のさらに詳しい構成を示すブロック図。

【図6】図1のディスク装置でデータ加工を行う方法を

示す説明図。

【図 7】図 1 のディスク装置のパスワード管理方法を示す説明図。

【図 8】図 1 のディスク装置のフラッシュメモリ内に格納されるデータを示す説明図。

【図 9】図 1 のディスク装置の動作を示すフローチャート。

【図 10】図 1 のディスク装置の動作を示すフローチャート。

【図 11】図 1 のディスク装置の動作を示すフローチャート。

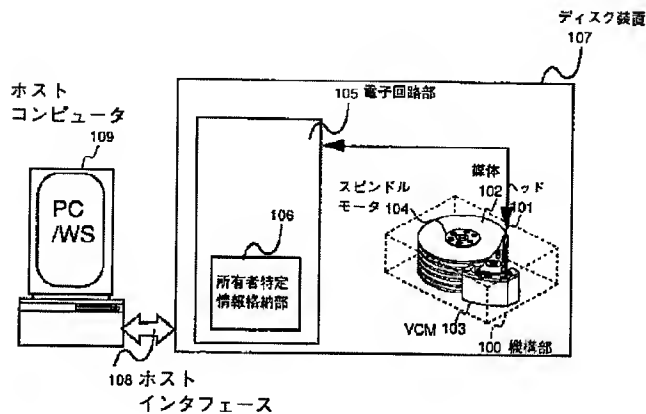
【図 12】図 1 のディスク装置の動作を示すフローチャート。

【図 13】図 1 のディスク装置の動作を示すフローチャート。

\*

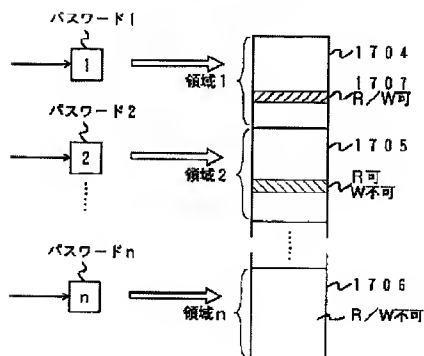
【図 1】

図 1



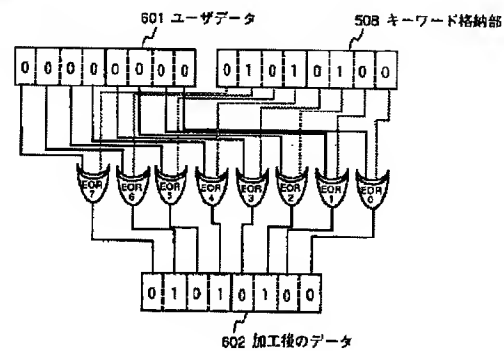
【図 7】

パスワードと領域関係図 (図 7)



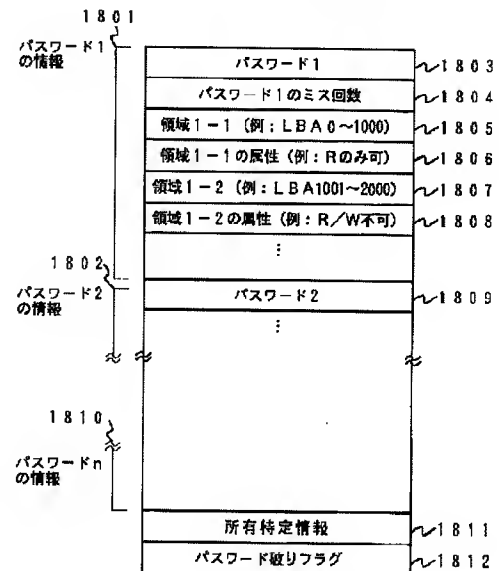
【図 6】

図 6

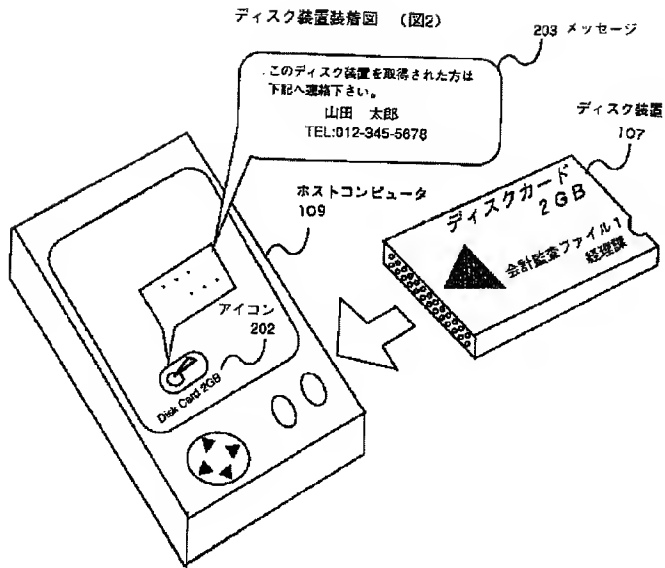


【図 8】

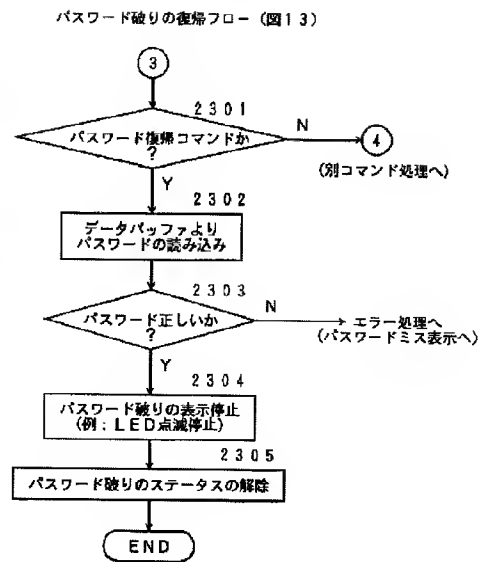
不揮発メモリ内のデータ (図 8)



【図2】

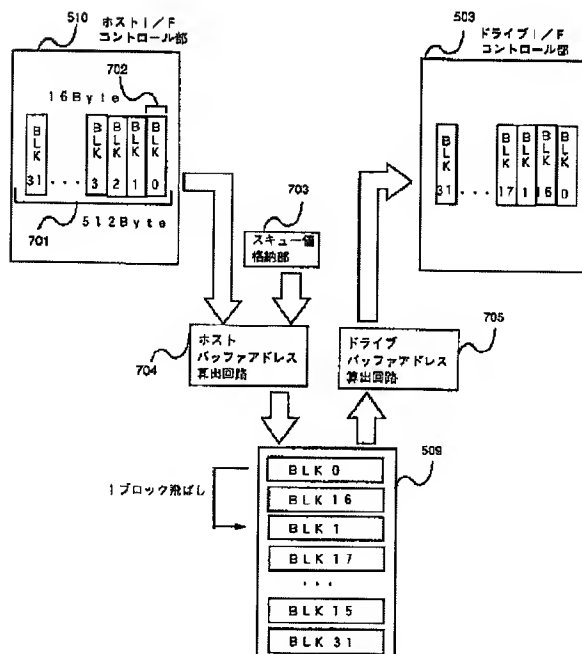


【図13】



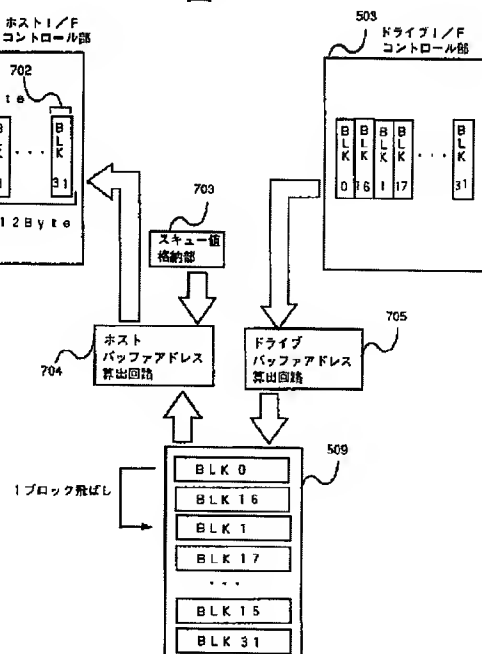
【図3】

図3

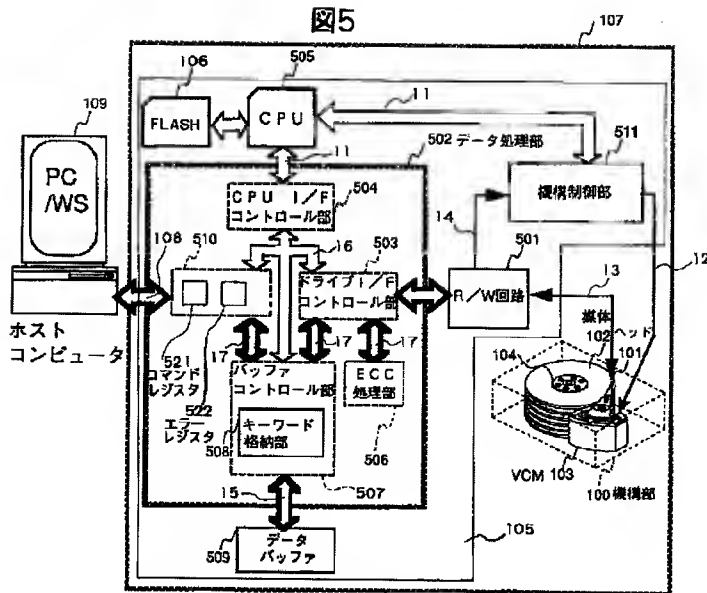


【図4】

図4

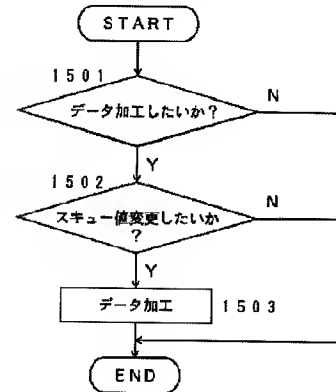


【図5】



【図15】

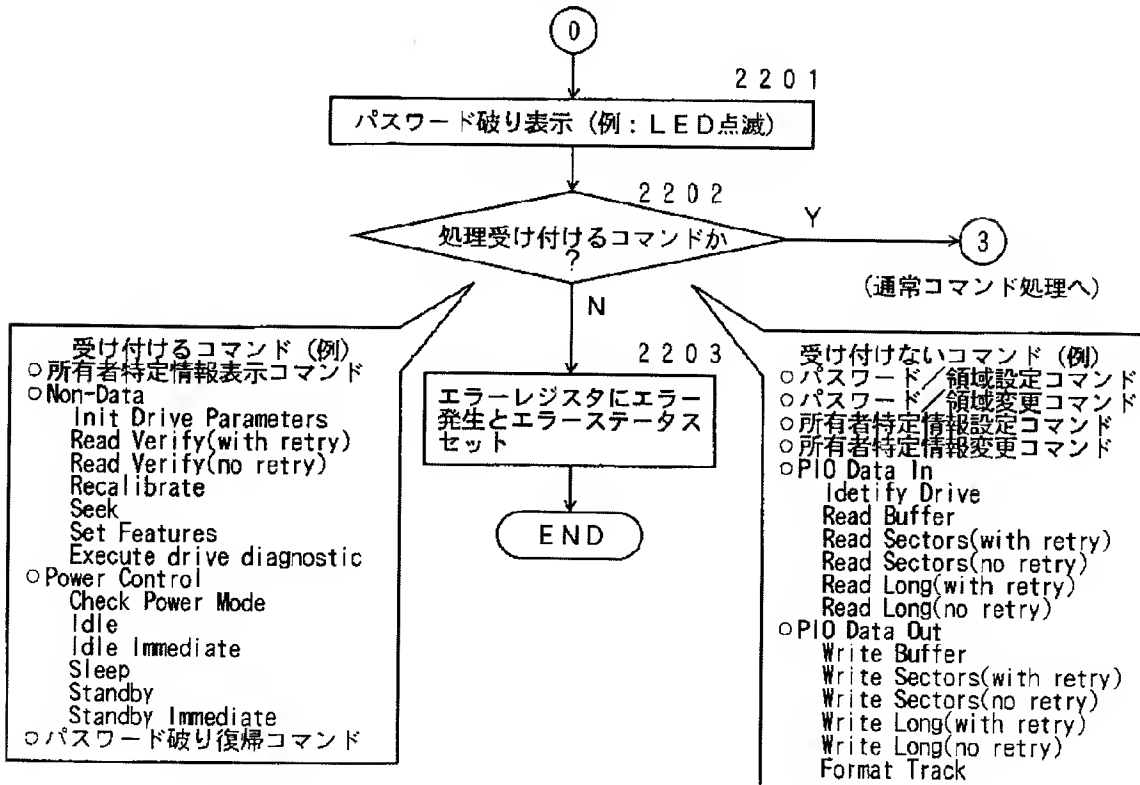
バッファデータ加工パラメータ設定フロー (図15)



【図12】

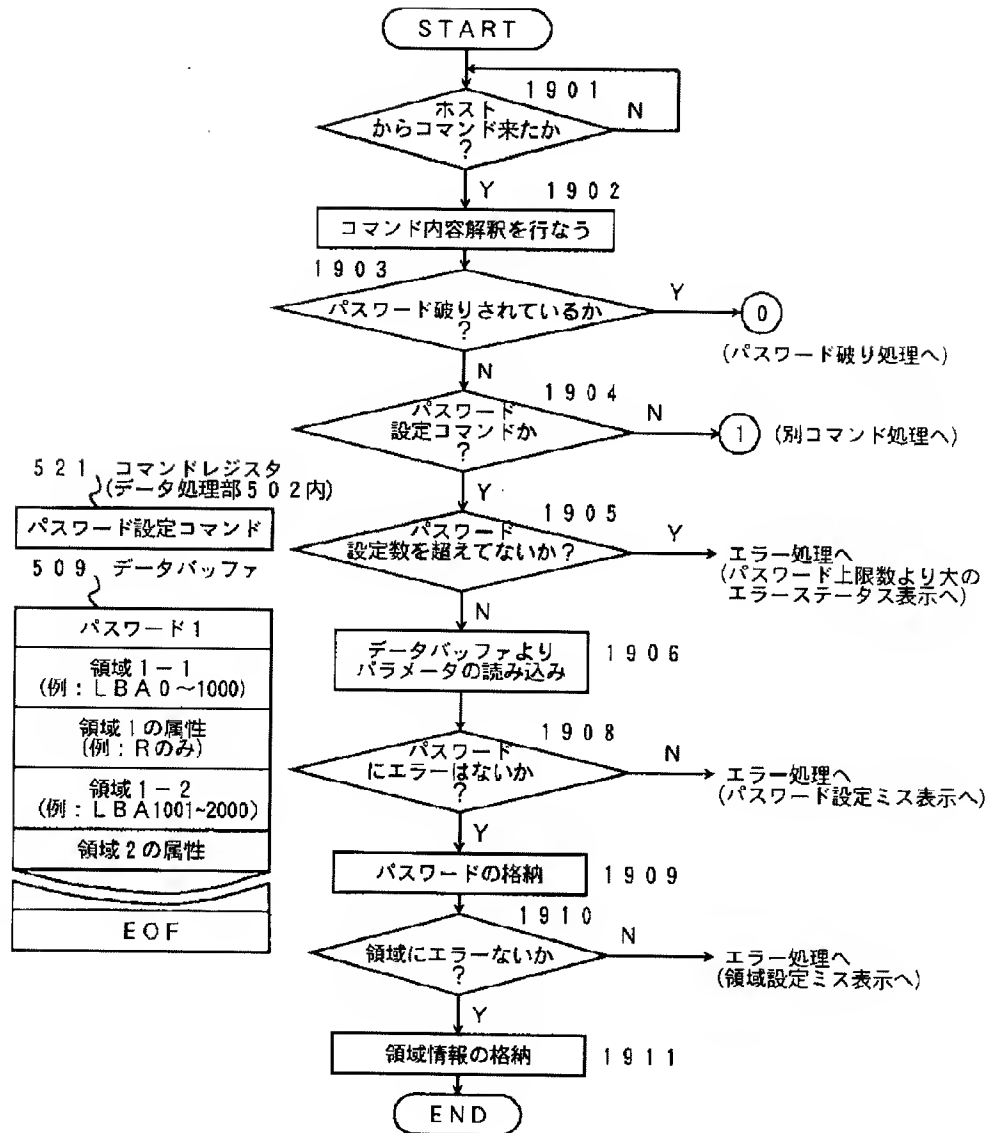
パスワード破り処理フロー (図12)

図19より



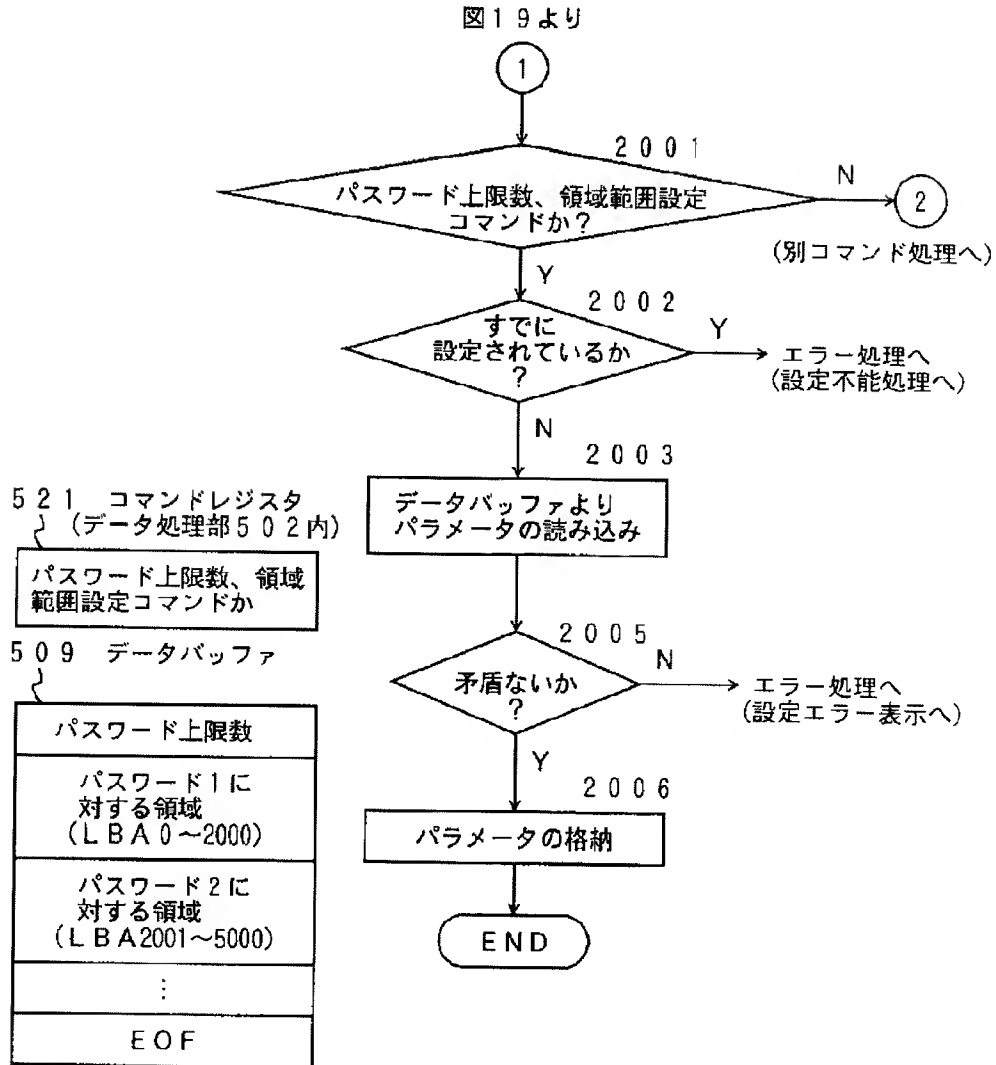
【図9】

図 9

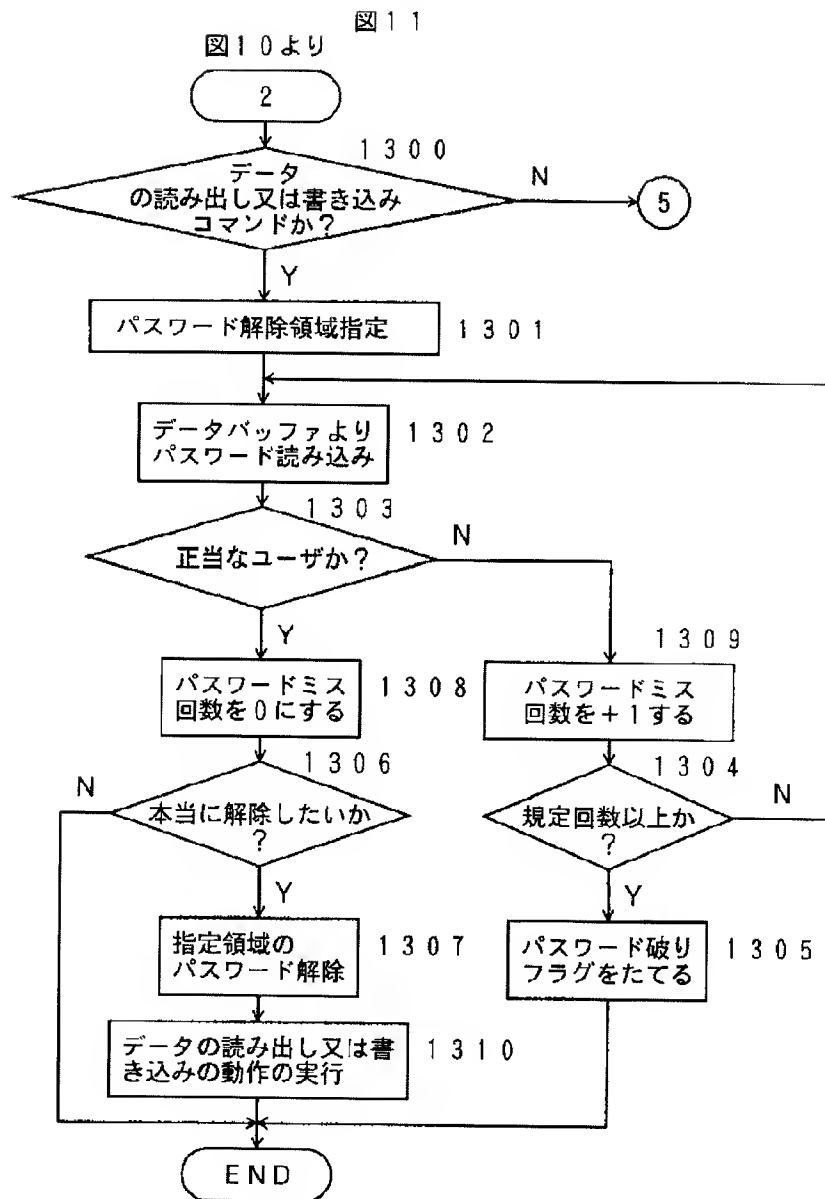


【図10】

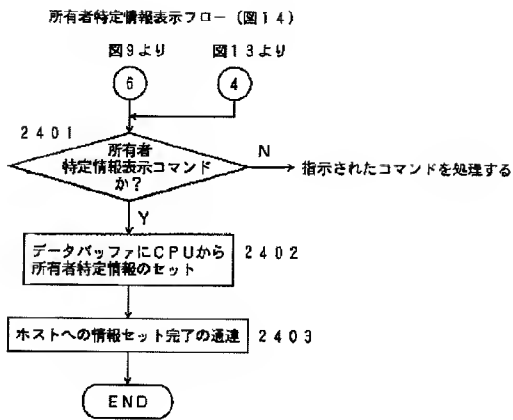
パスワード数、領域範囲設定フロー（図10）



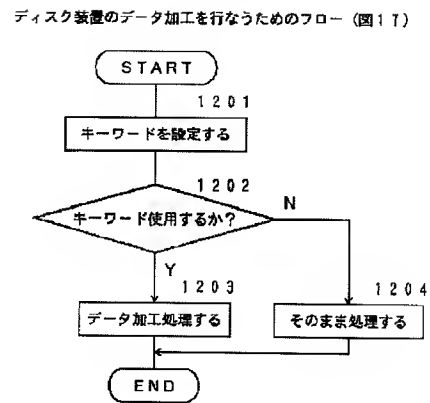
【図11】



【図14】



【図17】



【図16】

所有者特定情報登録消去フロー（図16）

